Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1 (Currently amended) A method for electronically delivering files over a public network of computers comprising at least one server node and multiple client nodes, the method comprising:

(a) enabling secure and reliable peer-to-peer file sharing between two client nodes by generating account information for a user, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key,

(i) in response to a file being selected for publication on a first client node by the user,

generating and associating a digital fingerprint with ~~a~~ the file, ~~in response to the file being selected for publication on a first client node~~

generating a bitstream ID for the file and including the bitstream ID in the fingerprint, and

using the user's private key to generate a digital signature from the file and including the digital signature in the fingerprint;

(ii) adding an entry for the file to a searchable index of shared files on the server node and storing the fingerprint on the server;

(iii) in response to a second client node selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node; and

(iv) authenticating the file by the second client node by generating a new bitstream ID, comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the digital signature ~~generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node~~ to determine the authenticity of the file and publisher.

2 (Original) The method of claim 1 further including the step of:

(b) enabling subscription-based decentralized file downloads to the client nodes by

(i) allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

(ii) when providing a current subscribing client node with the file, locating the closest client node containing the file, and

(iii) transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

3 (Canceled).

4 (Canceled).

5 (Canceled).

6 (Canceled).

7 (Currently amended) The method of claim ~~6~~ 1 wherein step (a)(ii) further includes the step of providing the server node with a database for storing the user's account information and the fingerprint for the file.

8 (Original) The method of claim 1 wherein step (a)(iii) further includes the step of transferring the file from the first client node directly to the second client node if both the first and second client nodes are logged-in to the network and no firewall separates the first and second client nodes.

9 (Original) The method of claim 8 wherein step (a)(iii) further includes the step of: if the second client node is not logged into the network, then temporarily storing the file on the server node, and delivering the file by the server node when second client node logs-in to the network.

10 (Original) The method of claim 9 wherein step (a)(iii) further includes the step of: if a firewall separates the first client node from the second client node, then using the server node to act as a proxy for the second client node and sending the file through the server node.

11 (Original) The method of claim 10 further including step (c) for allowing a user of the first client node to search for files on the network, and presorting results based on files found that are stored on client nodes located closest to the first client node.

12 (Currently amended) The method of claim ~~0~~ 11 wherein step (b)(iii) further includes the step of transferring the file during off-peak hours to take advantage of idle bandwidth of the subscribing node and thereby evening out bandwidth distribution of the network.

13 (Original) The method of claim 1 wherein step (a)(i) further includes the step of allowing a user of the first client node to privately publish the file or publicly publish the file.

14 (Original) The method of claim 1 wherein step (a)(ii) further includes transferring a copy of the file from the first node to the server node so that should the first node be off-line when another node request the file, the file may then be served by the server node.

15 (Original) The method of claim 1 wherein step (a)(iii) of transferring the file to the second client node further includes the step of transferring different portions of the file from different nodes and then reassembling the file upon receipt.

16 (Currently amended) A peer-to-peer file delivery network, comprising:

at least one server node;

multiple client nodes coupled to the server node over the network, each of the client nodes running a client application, wherein the client application works and operates in conjunction with the server node to

enable secure and reliable peer-to-peer file sharing between two client nodes by,

generating account information for a user of each client node, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key,

in response to a file being selected for publication on a first client node by a first user,

generating and associating a digital fingerprint with ~~a~~ the file ~~in response to the file being selected for publication on a first client node~~,

generating a bitstream ID for the file and including the bitstream ID in the fingerprint, and

using the user's private key to generate a digital signature from the file and including the digital signature in the fingerprint.

adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

in response to a second client node selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

authenticating the file by the second client node by generating a new bitstream ID, comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the

digital signature ~~generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node~~ to determine the authenticity and reliability of the file and publisher.

17 (Original) The network of claim 16 wherein the client application operates in conjunction with the server node to enable subscription-based decentralized file downloads to the client nodes by

allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

when providing a current subscribing client node with the file, locating the closest client node containing the file, and

transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

18 (Canceled).

19 (Canceled).

20 (Canceled).

21 (Canceled).

22 (Currently amended) The network of claim ~~21~~ 16 wherein the server node includes a database for storing the user's account information and the fingerprint for the file.

23 (Original) The network of claim 16 wherein the file is transferred from the first client node directly to the second client node if both the first and second client nodes are logged-in to the network and no firewall separates the first and second client nodes.

24 (Currently amended) The network of claim ~~0~~23 wherein if the second client node is not logged into the network, the file is temporarily stored on the server node and delivered the file by the server node when second client node logs-in to the network.

25 (Original) The network of claim 24 wherein if a firewall separates the first client node from the second client node, then the server node acts as a proxy for the second client node and sending the file through the server node.

26 (Original) The network of claim 25 wherein a user of the first client node may search for files on the network, and the results are presorted based on files found that are stored on client nodes located closest to the first client node.

27 (Original) The network of claim 26 wherein the file is transferred during off-peak hours to take advantage of idle bandwidth of the subscribing node and thereby evening out bandwidth distribution of the network.

28 (Original) The network of claim 16 wherein a user of the first client node may privately publish the file or publicly publish the file.

29 (Original) The network of claim 16 wherein a copy of the file is transferred from the first node to the server node so that should the first node be off-line when another node requests the file, the file may then be served by the server node.

30 (Original) The network of claim 16 wherein different portions of the file are transferred the second client from different client nodes and then reassembled the file upon receipt.

31 (Previously Presented) A method for electronically delivering files over a public network of computers comprising at least one server node and multiple client nodes, the method comprising:

(a) enabling secure and reliable peer-to-peer file sharing between two client nodes by,

(i) generating and associating a digital fingerprint with a file in response to the file being selected for publication on a first client node,

(ii) adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

(iii) in response to a second client node selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

(iv) generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher; and

(b) enabling subscription-based decentralized file downloads to the client nodes by

(i) allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

(ii) when providing a current subscribing client node with the file, locating the closest client node containing the file, and

(iii) transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

32 (Previously Presented) A peer-to-peer file delivery network, comprising:

at least one server node;

multiple client nodes coupled to the server node over the network, each of the client nodes running a client application, wherein the client application works and operates in conjunction with the server node to

enable secure and reliable peer-to-peer file sharing between two client nodes by, generating and associating a digital fingerprint with a file in response to the file

being selected for publication on a first client node,

adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

in response to a second client node selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity and reliability of the file and publisher; and

enable subscription-based decentralized file downloads to the client nodes by

allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

when providing a current subscribing client node with the file, locating the closest client node containing the file, and

transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.